

Exhibit A



03/31/2025

CT Log Number 548774657

Service of Process Transmittal Summary

TO: Allison Cotton
Chord Specialty Dental Partners
300 WILLOWBROOK LN STE 330
WEST CHESTER, PA 19382-5594

RE: Process Served in Pennsylvania

FOR: CDHA MANAGEMENT, LLC (Domestic State: DE)

ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:

TITLE OF ACTION: CHRISTINA FIGUEROA, as parent and natural guardian for A.A., A.F., and A.A., on behalf of herself and all others similarly situated vs. CDHA MANAGEMENT, LLC

CASE #: 202503720

PROCESS SERVED ON: C T Corporation System, Harrisburg, PA

DATE/METHOD OF SERVICE: By Traceable Mail on 03/31/2025

JURISDICTION SERVED: Pennsylvania

ACTION ITEMS: CT will retain the current log
Image SOP
Email Notification, Allison Cotton acotton@sparkdentalmanagement.com
Email Notification, Ilanna Perkins iperkins@chordsdp.com
Email Notification, Spark DSO - General Legal legal@chordsdp.com

REGISTERED AGENT CONTACT: C T Corporation System
600 N. 2nd Street, Suite 401
Harrisburg, PA 17101
877-467-3525
SmallBusinessTeam@wolterskluwer.com

REMARKS: Please note: That the documents reference 2 entity names. Since the delivery instructions are the same for both CT accepted process on behalf of the first named entity.

The information contained in this Transmittal is provided by CT for quick reference only. It does not constitute a legal opinion, and should not otherwise be relied on, as to the nature of action, the amount of damages, the answer date, or any other information contained in the included documents. The recipient(s) of this form is responsible for reviewing and interpreting the included documents and taking appropriate action, including consulting with its legal and other advisors as necessary. CT disclaims all liability for the information contained in this form, including for any omissions or inaccuracies that may be contained therein.

FIRST-CLASS



US POSTAGE PAID BY PITNEY BOWES
ZIP 19103 \$012.38⁰
02 7W
0008033962 MAR 28 2025

FIRST CLASS MAIL

PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT
OF THE RETURN ADDRESS, FOLD AT DOTTED LINE

CERTIFIED MAIL®



9589 0710 5270 1619 7357 55

GOLOMB LEGAL

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW

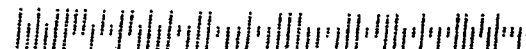
130 North 18th Street, Suite 1600, Philadelphia, PA 19103

CT Corporation System
600 North Second Street
Suite 401
Harrisburg, PA 17101



www.golomblegal.com

25-0001





GOLOMB LEGAL

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW

130 North 18th Street, Suite 1600
Philadelphia, PA 19103
Phone: 215-985-9177
Fax: 215-985-4169
www.golomblegal.com

Kevin Fay
kfay@golomblegal.com

March 28, 2025

CT Corporation System
600 North Second Street
Suite 401
Harrisburg, PA 17101

**RE: Figueroa, et al. v. CDHA Management, LLC, et al.
 CCP, Philadelphia County, March Term, 2025, No. 03720**

Dear Sir/Madam:

Enclosed please find a Civil Action Complaint which has been filed against you in the Court of Common Pleas, Philadelphia County relative to the above-captioned matter.

Please be advised that you have twenty (20) days to respond to the enclosed Complaint.

Thank you.

Sincerely,

Kevin Fay, Esquire
GOLOMB LEGAL, P.C.

KF/sl

Enclosure

****VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED****

9589 0710 5270 1619 7357 55

Court of Common Pleas of Philadelphia County
Trial Division**Civil Cover Sheet**

For Prothonotary Use Only (Docket Number)	
MARCH 2025	03720
E-Filed Number: 2503062230	

PLAINTIFF'S NAME CHRISTINA FIGUEROA		DEFENDANT'S NAME CDHA MANAGEMENT, LLC	
PLAINTIFF'S ADDRESS 3065 MEMPHIS STREET PHILADELPHIA PA 19134		DEFENDANT'S ADDRESS 300 WILLOWBROOK LANE SUITE 330 WEST CHESTER PA 19382	
PLAINTIFF'S NAME		DEFENDANT'S NAME SPARK DSO, LLC, ALIAS: CHORD SPECIALTY DENTAL PARTNERS (CHORD)	
PLAINTIFF'S ADDRESS		DEFENDANT'S ADDRESS 300 WILLOWBROOK LANE SUITE 330 WEST CHESTER PA 19382	
PLAINTIFF'S NAME		DEFENDANT'S NAME	
PLAINTIFF'S ADDRESS		DEFENDANT'S ADDRESS	
TOTAL NUMBER OF PLAINTIFFS 1	TOTAL NUMBER OF DEFENDANTS 2	COMMENCEMENT OF ACTION <input checked="" type="checkbox"/> Complaint <input type="checkbox"/> Petition Action <input type="checkbox"/> Notice of Appeal <input type="checkbox"/> Writ of Summons <input checked="" type="checkbox"/> Transfer From Other Jurisdictions	
AMOUNT IN CONTROVERSY <input type="checkbox"/> \$50,000.00 or less <input checked="" type="checkbox"/> More than \$50,000.00	COURT PROGRAMS <input type="checkbox"/> Arbitration <input type="checkbox"/> Mass Tort <input type="checkbox"/> Jury <input type="checkbox"/> Savings Action <input type="checkbox"/> Non-Jury <input type="checkbox"/> Petition <input checked="" type="checkbox"/> Other: CLASS ACTION		
CASE TYPE AND CODE C1 - CLASS ACTION			
STATUTORY BASIS FOR CAUSE OF ACTION			
RELATED PENDING CASES (LIST BY CASE CAPTION AND DOCKET NUMBER)		IS CASE SUBJECT TO COORDINATION ORDER? YES NO	
NAME OF PLAINTIFF'S/PETITIONER'S/APPELLANT'S ATTORNEY KEVIN W. FAY		ADDRESS GOLOMB LEGAL, PC 130 N. 18TH STREET SUITE 1600 PHILADELPHIA PA 19103	
PHONE NUMBER (215) 985-9177	FAX NUMBER (215) 985-4169	E-MAIL ADDRESS kfay@golomblegal.com	
SUPREME COURT IDENTIFICATION NO. 308252		DATE SUBMITTED Thursday, March 27, 2025, 11:35 am	
SIGNATURE OF FILING ATTORNEY OR PARTY KEVIN FAY			

TO THE PROTHONOTARY:

Kindly enter my appearance on behalf of Plaintiff/Petitioner/Appellant: CHRISTINA FIGUEROA

Papers may be served at the address set forth below.

FILED
PROPROTHY
MAR 27 2025
C. SMITH

GOLOMB LEGAL, P.C. RICHARD M. GOLOMB, ESQUIRE Identification No: 42845 KEVIN FAY, ESQUIRE Identification No.: 308252 One Logan Square 130 N. 18th Street, #1600 Philadelphia, PA 19103 Tel: (215) 608-9645 Fax: (215) 735-2211	MAJOR JURY CASE <i>Filed and Attested by the Office of the Clerk of the Court</i> CLASS ACTION ASSESSMENT OF DAMAGES REQUIRED Attorneys for Plaintiff and the Class
CHRISTINA FIGUEROA , as parent and natural guardian for A.A., A.F., and A.A., on behalf of herself and all others similarly situated, <p style="text-align: center;">Plaintiffs,</p> <p style="text-align: center;">v.</p> CDHA MANAGEMENT, LLC and SPARK DSO, LLC d/b/a CHORD SPECIALTY DENTAL PARTNERS <p style="text-align: center;">Defendants.</p>	COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY CIVIL ACTION -- CLASS ACTION JURY TRIAL DEMANDED No:

CLASS ACTION COMPLAINT

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP

Lawyer Reference Service
 Philadelphia Bar Association
 1101 Market Street, 11th Floor
 Philadelphia, PA 19107
 (215) 238-6300

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hacen falta asentar una comparencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o notificacion. Ademas, la corte puede decidir a favor del demandante y requiere que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades y otros derechos importantes para usted.

LLEVE ESTA DEMANDA A UN ABOGADO INMEDIATAMENTE. SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICIO. VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.

Lawyer Reference Service
 Philadelphia Bar Association
 1101 Market Street, 11th Floor
 Philadelphia, PA 19107
 (215) 238-6300

Plaintiff Christina Figueroa (“Plaintiff”) brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendants, CDHA MANAGEMENT, LLC and SPARK DSO, LLC d/b/a CHORD SPECIALTY DENTAL PARTNERS (“Defendants”), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information (“PII”) and protected health information (“PHI”) owe a duty to the individuals to whom that data relates, including patients and employees. This duty arises based upon the parties’ relationship and because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person’s PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

3. As a healthcare provider and vendor for a healthcare provider, Defendants are required by law to provide every patient with a Notice of Privacy Practices.

4. Defendants knowingly obtain patient’s PII and PHI and has a resulting duty to securely maintain such information in confidence.

5. Plaintiff brings this class action on behalf of individuals and patients of Defendants, or otherwise people that are customers of or have their records collected by Defendants, whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach that was first announced by Defendants on March 14, 2025 (the “Data Breach”).

6. On or about September 11, 2024, Defendants discovered suspicious activity related to an employee’s email account. Upon investigating, Defendants determined that an unauthorized individual had gained access to several accounts between August 19, 2024 and September 25, 2024.

7. Defendants determined that the PII and/or PHI of Plaintiff’s children and other class members had been accessed.

8. Despite the fact that Defendants became aware of the Data Breach on September 11, 2024, they failed to notify the Plaintiff and the putative Class Members until March 14, 2025.

9. Plaintiff, as parent and natural guardian of her children, A.A., A.F., and A.A., on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty/confidence, breach of implied contract, unjust enrichment, and declaratory judgment, seeking actual and punitive damages, with attorneys’ fees, costs, and expenses, and appropriate injunctive and declaratory relief.

10. Based on the public statements of Defendants to date, a wide variety of PII and PHI was implicated in the breach. This includes the following: name, address, social security number, driver’s license, bank account information, payment card information, date of birth, medical information, and health insurance information.

11. As a direct and proximate result of Defendants’ inadequate data security, their breach of duty to handle PII and PHI with reasonable care, and their failure to maintain the

confidentiality of patients' medical records and PHI, Plaintiff's and Class Members' PII and/or PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

12. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

13. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, along with declaratory judgment and injunctive relief requiring Defendant to, at minimum: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

14. Plaintiff Christina Figueroa is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff's children's PHI and PII records were maintained within Defendants' networks, as Plaintiff's children received healthcare services from Defendants. Shortly after March 14, 2025, Plaintiff received a notice letter from Defendants informing Plaintiff that her children's PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach, including but not limited to their names and health insurance information.

15. Defendant CDHA Management, LLC (“CDHA”) is a Delaware limited liability company with its principal place of business located at 300 Willowbrook Lane, Suite 330, West Chester, Pennsylvania 19382. Upon information and belief, CDHA provides administrative and support services for co-defendant Spark DSO, LLC d/b/a Chord Specialty Dental Partners.

16. Defendant Spark DSO, LLC d/b/a Chord Specialty Dental Partners (“Chord”) is a Pennsylvania limited liability company with its principal place of business located at 300 Willowbrook Lane, Suite 330, West Chester, Pennsylvania 19382. Chord is a healthcare provider with corporate offices in Nashville, TN and serves various communities in Pennsylvania, as well as states in the Mid-Atlantic and Mid-South.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this matter pursuant to 42 Pa. Cons. Stat. § 931 and 42 Pa. Cons. Stat. § 5301, as Plaintiff was and is a citizen of Pennsylvania at the time of the Data Breach. This Court also has jurisdiction over this action as Defendant Chord is a Pennsylvania limited liability company, and both Defendants continuously and systematically operate and conduct business in Philadelphia County, and all the relevant incidents involved in this matter occurred in Pennsylvania.

18. Venue is proper in this Court pursuant to Pa. R. C. P. 2179 because Plaintiff resides in this County, the Defendants regularly conduct business in Philadelphia County, a substantial part of events, acts, and omissions giving rise to Plaintiff’s claims occurred in, was directed to, and/or emanated from this County.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

19. At all relevant times, Defendants knew they were storing and permitting their employees to use internal network servers to transmit valuable, sensitive PII and PHI and that, as a result, Defendants' systems would be attractive targets for criminals and/or cybercriminals.

20. Defendants also knew that any breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

21. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others. Healthcare companies have been targeted most recently including the Kaiser Foundation Health Plan, HCA Healthcare, and Managed Care of North America (MCNA Dental), to name a few.

22. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."¹ PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

23. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the IRTC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-

¹ Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/>.

sensitive” records.²

24. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to \$1.7 billion in 2018.³

25. The healthcare industry has become a prime target for threat actors: “High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.”⁴

26. “Hospitals store an incredible amount of patient data. Confidential data that’s worth a lot of money to hackers who can sell it on easily – making the industry a growing target.”⁵

27. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant’s patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

28. As indicated by Jim Trainor, second in command at the FBI’s cyber security division: “Medical records are a gold mine for criminals—they can access a patient’s name, DOB, Social Security and insurance numbers, and even financial information all in one place.

² *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, available at <https://notified.idtheftcenter.org/s/resource#annualReportSection>.

³ Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at [https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20\(1\)](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1)).

⁴ <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>.

⁵ *Id.*

Credit cards can be, say, five dollars or more where PHI records can go from \$20 say up to—we've even seen \$60 or \$70.”⁶ A complete identity theft kit that includes health insurance credentials may be worth up to \$1,000 on the black market, whereas stolen payment card information sells for about \$1.⁷

29. According to Experian:

Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

ID theft victims often have to spend money to fix problems related to having their data stolen, which averages \$600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly \$13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.⁸

⁶ IDEXperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: <https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>.

⁷ PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.

⁸ Experian, Healthcare Data Breach: What to Know About them and What to Do After One: <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

30. The “high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to \$1,000 online.**”⁹

31. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”¹⁰

32. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its PII and PHI

33. On September 11, 2024, Defendants discovered suspicious activity related to an employee’s email account. Upon investigating, Defendants determined that an unauthorized individual had gained access to several accounts between August 19, 2024 and September 25, 2024.

⁹ <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

¹⁰ United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: <https://www.gao.gov/assets/gao-07-737.pdf>.

34. According to Defendants, they conducted an investigation and determined that personal information of patients, including minors, was affected by the Data Breach.

35. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures, and their failure to follow their own policies, in order to protect its patients' PII and PHI.

36. Plaintiff received the notice from Defendants dated March 14, 2025, advising that Plaintiff's children were victims of Defendants' data security failures exposing PHI and PII. A copy of the Notice is attached as Exhibit A.

37. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

38. In its notice to Plaintiff and Class members, Defendant asserted: "[w]e take the privacy and security of all information in our care seriously."

39. The notice letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendants completed their investigation, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendants know if the data has been further disseminated.

40. Defendants acknowledge that they are responsible to safeguard Plaintiff and Class Members' PHI and PII. They pledge that they take privacy very seriously and make numerous promises that they will maintain the security and privacy of PHI and PII.

41. Patients who receive healthcare services, such as Plaintiff, entrusted their PHI and PII to Defendants with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff and Class Members' PHI and PII from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Defendants to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. Defendants were well aware that the PHI and PII they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.¹¹ Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

45. The ramifications of Defendant's failure to keep PHI and PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

46. Further, criminals often trade stolen PHI and PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI and PII on the internet, thereby making such information publicly available.

¹¹ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited March 26, 2025).

47. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.¹² This time lag between when harm occurs versus when it is discovered, and also between when PHI and PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

48. Defendants knew, or should have known, the importance of safeguarding PHI and PII entrusted to them and of the foreseeable consequences if their systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

49. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI and/or PII.

50. Despite all of the publicly available knowledge of the continued compromises of PHI and PII, Defendants' approach to maintaining the privacy of the PHI and PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

51. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendants' misfeasance.

¹² *Identity Theft and Your Social Security Number*, Social Security Administrative, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed March 26, 2025).

52. Once PHI and PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

53. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

54. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PII and/or PHI;
- c. The loss of the opportunity to control how their PII and/or PHI is used;
- d. The diminution in value of their PII and/or PHI;
- e. The compromise, publication, and/or theft of their PII and/or PHI;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;

- j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
- k. The continued risk to their PII and/or PHI, which remains in the possession of Defendants and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII and/or PHI in their possession; and
- l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

55. To date, Defendants have not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, they has taken to secure the PHI and PII still in their possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Defendants have proper measures in place to prevent another breach from occurring in the future.

56. Defendants were expressly prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

57. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹³

¹³ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed March 26, 2025).

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.¹⁴ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendants failed to properly implement basic data security practices. Their failure to employ reasonable and appropriate measures to protect against unauthorized access to PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

61. Defendants were at all times fully aware of their obligation to protect PHI and PII and were also aware of the significant repercussions that would result from their failure to do so.

C. Plaintiff and Class Members Suffered Damages

62. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to:

- 1) closely monitor their medical statements, bills, records, and credit and financial accounts;
- 2) change login and password information on any sensitive account even more frequently than

¹⁴ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed March 26, 2025).

they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

63. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

64. As a result of Defendants' failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

65. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.¹⁵

66. With respect to health care breaches, another study found “the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft.”¹⁶

67. “Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial

¹⁵ <https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud>.

¹⁶ <https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud>.

fraud to crafting of bespoke phishing lures.”¹⁷

68. The reality is that cybercriminals seek nefarious outcomes from a data breach” and “stolen health data can be used to carry out a variety of crimes.”¹⁸

69. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.¹⁹

70. “Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous.”²⁰

71. Plaintiff and the Class members have also been injured by Defendant’s unauthorized disclosure of their confidential and private medical records and PHI.

72. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants’ systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their patients’ PII and PHI.

¹⁷ *Id.*

¹⁸ <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

¹⁹ *Id.*

²⁰ <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>.

CLASS ALLEGATIONS

73. Plaintiff brings this case individually and, pursuant to Rule 1702 of the Pennsylvania Rules of Civil Procedure, on behalf of the following classes:

Nationwide Class

All individuals in the United States whose PII and/or PHI was maintained by the Defendants and who were sent a notice of the Data Breach.

Pennsylvania Sub Class

All individuals in Pennsylvania whose PII and/or PHI was maintained by the Defendants and who were sent a notice of the Data Breach.

74. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

75. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

76. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the files implicated in the Data Breach. Based on information and belief, the Class includes thousands of individuals.

77. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

- a. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendants had a duty to maintain the confidentiality of Plaintiff and Class Members' PHI;
- c. Whether Defendants breached their obligation to maintain Plaintiff and the Class members' medical information in confidence;
- d. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached their duties thereby;
- e. Whether Defendants breached their fiduciary duty to Plaintiff and the Class.
- f. Whether Defendants failed to properly give notice under relevant law;
- g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;
- h. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendants' wrongful conduct; and
- i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

78. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendants to safeguard PII and PHI. Plaintiff and Class Members all entrusted their PII and PHI to Defendants, and each of them had their PII and PHI obtained by an unauthorized third party.

79. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

80. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their common law and statutory duties to secure PII and PHI on their network servers, then Plaintiff and each Class Member suffered damages from the exposure of their sensitive personal information in the Data Breach.

81. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

82. **Manageability.** While the precise size of the Class is unknown without the disclosure of Defendants' records, it is likely there are at least thousands of individuals whose PII and/or PHI was compromised in the Data Breach. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE and NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

83. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

84. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

85. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

86. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

87. Defendants' duty also arose from Defendants' position as a provider of healthcare and an administrator. Defendants hold themselves out as trusted providers of healthcare and administrative services, and thereby assume a duty to reasonably protect their patients' information. Indeed, Defendants were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

88. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security,

confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow their own privacy policies and practices published to their patients.

89. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

90. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

91. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of their patients.

92. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

93. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

94. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act was intended to guard against.

95. Pursuant to Defendants' websites, they both acknowledged their legal duties by stating the following:

- a) "The privacy of your health information is important to us. We understand that your health information is personal, and we are committed to protecting it. This Notice describes how we may use and disclose your protected health information to carry out treatment, payment, or health care operations, and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. Protected health information is information about you, including demographic information, that may identify you and that relates to your past, present, or future physical or mental health or condition and related health care services."²¹
- b) "We are required by law to: (i) Maintain the privacy of your protected health information (ii) Give you this Notice of our legal duties and privacy practices with respect to that information (iii) Abid by the terms of our Notice that is currently in effect."²²
- c) "Right to Receive Notification of a Security Breach – We are required by law to notify you if the privacy or security of your health information has been breached. The notification will occur by first class mail within sixty (60) days of the event. A breach occurs when there has been an unauthorized use or disclosure under

²¹ See <https://www.chordsdp.com/privacy-policy/> (last visited March 26, 2025). See also https://cdhdental.wpenginepowered.com/wp-content/uploads/2025/01/CDH_Combined-Privacy-Packet.pdf (last visited March 26, 2025).

²² See *id.*

HIPAA that compromises the privacy or security of your health information. The breach notification will contain the following information: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach; (2) the steps you should take to protect yourself from potential harm resulting from the breach; and (3) a brief description of what we are doing to investigate the breach, mitigate losses, and to protect against further breaches.”²³

96. Defendants violated their own policies by actively disclosing Plaintiff’s and the Class Members’ PII and/or PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff’s and Class Members’ PII and/or PHI; failing to maintain the confidentiality of Plaintiff’s and the Class Members’ records; and by failing to provide timely notice of the breach of PII and/or PHI to Plaintiff and the Class.

97. As a direct and proximate result of Defendants’ negligence, Plaintiff and Class Members have suffered injuries, including:

- a. Theft of their PII and/or PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

²³ See *id.*

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PII and/or PHI;

j. The erosion of the essential and confidential relationship between Defendants – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

98. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Classes)

99. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

100. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

101. As a healthcare provider, Defendants have a fiduciary relationship to their patients, like Plaintiff and the Class Members.

102. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII and PHI related to Plaintiff and the Class, which they were required to maintain in confidence.

103. Defendants owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

104. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the information within Plaintiff and the Class members' medical records.

105. Patients like Plaintiff and Class members have a privacy interest in personal medical matters, and Defendants had a fiduciary duty not to disclose medical data concerning patients.

106. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII and PHI of Plaintiff and Class members, information not generally known.

107. Plaintiff and Class Members did not consent to nor authorize Defendants to release or disclose their PHI to an unknown criminal actor.

108. Defendants breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security programs in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their patients and customers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' PHI and medical records/information to a criminal third party.

109. But for Defendants' wrongful breach of their fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

110. As a direct and proximate result of Defendants' breach of their fiduciary duties and breach of their confidences, Plaintiff and Class Members have suffered injuries, including:

- a. Theft of their PII and/or PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
- g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendants – as a health care services providers – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendants.

111. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

112. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

113. When Plaintiff and members of the Class provided their personal information to Defendants, Plaintiff and members of the Class entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

114. Defendants required Plaintiff and class members to provide and entrust their PHI and PII and financial information as a condition of obtaining Defendants' services.

115. Plaintiff and Class members would not have provided and entrusted their PHI and PII and financial information to Defendants in the absence of the implied contract between them and Defendants.

116. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendants.

117. Defendants breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

118. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

119. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

120. This count is brought in the alternative to Plaintiff's breach of contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

121. Plaintiff and Class members conferred a benefit on Defendants by way of customers' paying Defendants to maintain Plaintiff and Class members' personal information.

122. The monies paid to Defendants were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

123. Defendants failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result Defendants were overpaid.

124. Under principles of equity and good conscience, Defendants should not be permitted to retain the money because Defendants failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

125. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

126. Defendants' enrichment at the expense of Plaintiff and Class members is and was unjust.

127. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

128. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

129. Under the Pennsylvania Declaratory Judgments Act, 42 Pa. C.S. § 7531, *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations

shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

130. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate, contrary to Defendants' assertion that it has confirmed the security of its network. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

131. Pursuant to its authority under the Declaratory Judgments Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants owe a legal duty to secure PII and PHI and to timely notify employees, patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and
- b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure PII and PHI.

132. This Court also should issue corresponding prospective injunctive relief requiring Defendants to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Plaintiff and Class members' PII and PHI possessed by Defendants; and 3) provide, at their own expense, all impacted victims

with lifetime identity theft protection services.

133. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

134. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

135. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, pray for relief as follows:

- a. For an order certifying the Class under the Pennsylvania Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

- c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;
- e. Declaratory and injunctive relief as described herein;
- f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- g. Awarding pre- and post-judgment interest on any amounts awarded; and
- h. Awarding such other and further relief as may be just and proper.

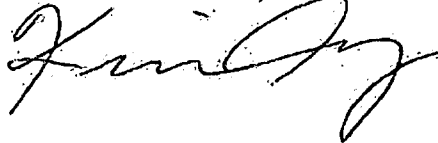
JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: March 27, 2025

Respectfully Submitted,

GOLOMB LEGAL, P.C.



BY: RICHARD M. GOLOMB, ESQ.

KEVIN FAY, ESQ.

Identification Nos.: 42845, 308252

One Logan Square

130 N. 18th Street, #1600

Philadelphia, Pennsylvania 19103

Telephone: (215) 985-9177

rgolomb@golomblegal.com

kfay@golomblegal.com

Vinesign Document ID: 9990B8FD-0C68-43CC-81C9-F53449E4E4E4

VERIFICATION

CHRISTINA FIGUEROA hereby states that she is the Plaintiff in this action and verifies that the statements made in the foregoing **CIVIL ACTION COMPLAINT** are true and correct to the best of her knowledge, information and belief. The undersigned understands that the statements therein are made subject to penalties of 18 Pa. C.S. Section 4904 relating to unsworn falsification to authorities.



CHRISTINA FIGUEROA

Date: 03/26/2025

EXHIBIT "A"

CDHA Management, LLC and Spark DSO, LLC dba Chord Specialty Dental Partners
c/o Cyberscout
PO Box 1258
Dearborn, MI 48120-8598



PL021A00205649
Parent or Guardian of

3065 MEMPHIS STREET
PHILADELPHIA, PA 19134-4322

[REDACTED]

March 14, 2025

Dear Parent or Guardian of Ariella Aponte:

CDHA Management, LLC and Spark DSO, LLC dba Chord Specialty Dental Partners ("Chord") write to inform you of an incident that may have involved some of your minor's information described below. We take the privacy and security of all information in our care seriously. While there is no indication that any information has been misused, we are providing information about the event and steps you can take to help protect your minor's information, should you feel it is appropriate to do so.

What Happened: On or about September 11, 2024, Chord discovered suspicious activity related to an employee's email account. Upon discovery, Chord took immediate action to secure the account and engaged a team of third-party specialists to investigate the incident. The investigation determined that an unauthorized individual had gained access to a few employees' email accounts for a limited time between August 19, 2024, and September 25, 2024. Chord then reviewed the contents of the email accounts to determine the types of information contained therein and to whom that information related. On February 19, 2025, following a thorough review, Chord confirmed that a limited amount of personal information may have been accessed by an unauthorized party in connection with this incident.

What Information Was Involved: The potentially accessed information may have included your minor's name in combination with health insurance information.

What We Are Doing: Chord has taken steps to address the event and is committed to protecting the information entrusted to its care. Upon learning of this event, Chord took steps to secure the email accounts and undertook a thorough investigation. Chord also implemented additional technical safeguards to further enhance the security of information in its possession and to prevent similar incidents from happening in the future. As an additional safeguard, Chord is offering your minor access to Cyber Monitoring services for you and your minor child for 12 months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: In addition to enrolling in the complimentary credit monitoring service detailed below, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your minor's credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your minor's accounts, please promptly change the password, contact the financial institution or company if applicable, and take any additional steps needed to protect your minor's account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General.

3/27/25, 11:35 AM

The Philadelphia Courts E-Filing, #2503062230 Submitted

**The Philadelphia Courts
Electronic Filing System**

March 27, 2025 11:35am

Welcome!

[View Preliminary Cover Sheet](#)

Kevin W. Fay

Username: **kfay**[Update Information](#)[Main Menu](#)[CP Civil Help](#)[Log Off](#)EFile #: **2503062230**Status: **Pending**Started: **03/27/25**Court: **CP**

* Required Field.

User Accepts/Agrees to [Rules/Agreement](#).☒ **CONTACT US****IMPORTANT NOTICE**

The legal paper you electronically presented for filing has been received by the Office of Judicial Records of Philadelphia County. The following information will assist you in tracking the status of the pleading:

Caption: **FIGUEROA VS CDHA MANAGEMENT, LLC ETAL**Date Presented to Office of Judicial Records for Filing: **March 27, 2025 11:35 AM**Type of Pleading/Legal Paper: **COMPLAINT**E-File No.: **2503062230**Confirmation No.: **4B703E806**Personal Reference No.: **25-0007**Filing Fee: **\$643.17**

The requisite filing fees will only be charged to your credit card upon acceptance of your legal paper by the Office of Judicial Records. No charge will be posted to your credit card if your legal paper is rejected.

Please be advised that the above legal paper will not be deemed to have been "filed" until it has been reviewed and accepted by the Office of Judicial Records. You will be notified by email when your legal paper has been approved or rejected by the Office of Judicial Records. If you do not receive an approval or rejection email within two (2) business days you may contact the Office of Judicial Records at (215) 686-6652 or OJRCivil@courts.phila.gov to determine the status of your electronic filing.

At any time, you may check the status of your electronic filing by logging in to the Electronic Filing Web Site at <http://courts.phila.gov> using the Court-issued User Name and Password.

You are reminded that Pa. O.C. Rule 4.7(c) requires that a hard copy of the legal paper you have filed electronically shall be signed and, as applicable, verified concurrently with the electronic filing of the legal paper, and shall be maintained by you for five (5) years after the final disposition of the case.

At the request of any party, you must produce for inspection the original or a hard copy of a legal paper or exhibit within fourteen (14) days, or the court may, upon motion, grant appropriate sanctions.

Thank You,
Eric Feder
Deputy Court Administrator
Director, Office of Judicial Records

DISCLAIMER

The First Judicial District will use your electronic mail address and other personal information only for purposes of Electronic Filing as authorized by Pa.R.C.P. No. 205.4 and Philadelphia Civil Rule *205.4.

Use of the Electronic Filing System constitutes an acknowledgment that the user has read the [Electronic Filing Rules](#) and [Disclaimer](#) and agrees to comply with same.

3/27/25, 11:35 AM

The Philadelphia Courts E-Filing, #2503062230 Submitted

[Go back to main menu](#)



Copyright ©2002-2008 First Judicial District of Pennsylvania. All Rights Reserved.